ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
30 июня 2025 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА ОЦЕНКИ УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

2025

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств (далее – Методика) разработана в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю (далее – ФСТЭК России), утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

2. Методика определяет порядок оценки уровня критичности уязвимостей, выявленных в программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, в том числе функционирующих на базе информационно-телекоммуникационной инфраструктуры центров обработки данных (далее – информационные системы).

3. Настоящая Методика подлежит применению операторами информационных систем при принятии ими мер по устранению уязвимостей программных, программно-аппаратных средств информационных систем в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, и требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, а также иными нормативными правовыми актами и методическими документами ФСТЭК России.[1]

4. Меры по устранению уязвимостей в сертифицированных программных, программно-аппаратных средствах защиты информации выполняются в сроки, установленные настоящей Методикой, с присвоением таким уязвимостям критического уровня ($V > 8,0$), а также в соответствии с эксплуатационной документацией на них и рекомендациями разработчика.

---

[1] Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденные приказом ФСТЭК России от 11 апреля 2025 г. № 117.

Требования к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых предприятиями оборонно-промышленного комплекса, утвержденные приказом ФСТЭК России от 28 февраля 2017 г. № 31.

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239.

Требования к обеспечению защиты информации в автоматизированных системах управления производственными процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2013 г. № 31.

5. В Методике используются термины и определения, установленные национальными стандартами ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей», ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем», иными национальными стандартами в области защиты информации и обеспечения информационной безопасности.

6. В связи с утверждением настоящей Методики не применяется для оценки уровня критичности уязвимостей программных, программно-аппаратных средств Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденная ФСТЭК России 28 октября 2022 г.

II. ПОРЯДОК ОЦЕНКИ УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

7. Уровень критичности уязвимостей оценивается в целях принятия обоснованного решения операторами информационных систем о необходимости устранения уязвимостей, выявленных в программных, программно-аппаратных средствах по результатам анализа уязвимостей в информационных системах.

8. Исходными данными для определения критичности уязвимостей являются:

а) база уязвимостей программного обеспечения, программно-аппаратных средств, содержащаяся в Банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), а также иные источники, содержащие сведения об известных уязвимостях;

б) официальные информационные ресурсы разработчиков программного обеспечения, программно-аппаратных средств и исследователей в области информационной безопасности;

в) сведения о составе и архитектуре информационных систем, полученные по результатам их инвентаризации и (или) приведенные в документации на информационные системы;

г) результаты контроля уровня защищенности информационных систем и содержащейся в них информации, проведенные оператором (в том числе тестирование на проникновение, учения (тренировки), мероприятия по проведению эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений, установленные Постановлением Правительства Российской Федерации от 26 марта 2025 г. № 372).

Указанные исходные данные могут уточняться или дополняться с учетом особенностей сферы деятельности, в которой функционируют информационные системы.

9. Оценка уровня критичности уязвимостей программных, программно-аппаратных средств проводится специалистами по защите информации.

10. В случае, если информационная система функционирует на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, то оценка уровня критичности уязвимостей программных, программно-аппаратных средств проводится с учетом используемой инфраструктуры центра обработки данных.

11. Оценка уровня критичности уязвимостей программных, программно-аппаратных средств применительно к информационным системам включает:

1) определение перечня программных, программно-аппаратных средств, подверженных уязвимостям;

2) определение мест установки программных, программно-аппаратных средств, подверженных уязвимостям (например, на периметре информационных систем, во внутреннем сегменте систем, при реализации критических процессов (бизнес-процессов) и других сегментах информационной системы);

3) расчет уровня критичности уязвимости программных, программно-аппаратных средств в системе (V).

12. Расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе V осуществляется по следующей формуле:

$$V = I_{cvss} \times I_{infr} \times \left(I_{at} + I_{imp} \right), \text{ где}$$

I_{cvss} – показатель, характеризующий уровень опасности уязвимости;

I_{infr} – показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационных систем;

I_{at} – показатель, характеризующий возможность эксплуатации уязвимости программных, программно-аппаратных средств в информационных системах;

I_{imp} - показатель, характеризующий последствия эксплуатации уязвимости программных, программно-аппаратных средств в информационных системах.

13. В качестве показателя I_{cvss} берется значение, рассчитанное разработчиком (вендором) программного обеспечения по базовым метрикам в соответствии с методикой Common Vulnerability Scoring System[2] (CVSS) 3.1, которая содержится в Банке данных угроз безопасности информации ФСТЭК России[3], а также иных известных базах данных уязвимостей. В случае отсутствия для уязвимости оценки уровня

[2] https://www.first.org/cvss.

[3] https://bdu.fstec.ru/calc31.

опасности по базовым метрикам в соответствии с методикой Common Vulnerability Scoring System (CVSS) 3.1, специалист самостоятельно определяет версию CVSS, по которой производится оценка критичности уязвимости.

14. Показатель I_{infr} определяется по следующей формуле:

$$I_{infr} = k \times K + l \times L + p \times P, \text{ где}$$

K – показатель, характеризующий тип компонента информационной системы[4], подверженного уязвимости;

L – показатель, характеризующий количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов);

P – показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы или периметра сегмента информационной системы (в случае сегментирования информационной системы);

k, l, p – весовые коэффициенты показателей (значения приведены в таблице 1 настоящей Методики).

15. В случае, если уязвимости подвержено несколько компонентов информационной системы (например, имеются сведения о подверженности уязвимости компонентов, обеспечивающих реализацию критических процессов, функций, полномочий, а также межсетевых экранов, сетевых устройств и шлюзов, автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации, систем хранения данных и других компонентов), то итоговой оценке показателя, характеризующего тип компонента информационной системы (K), присваивается наибольшее из значений.

16. Показатель I_{at} определяется в соответствии с имеющейся у оператора информацией о возможности эксплуатации уязвимости на момент оценки уровня критичности уязвимостей программных, программно-аппаратных средств по следующей формуле:

$$I_{at} = e \times E, \text{ где}$$

E – показатель, характеризующий эксплуатацию уязвимости нарушителями в реальных компьютерных атаках;

e – весовой коэффициент для показателя E (значения приведены в таблице 1 настоящей Методики).

---

[4] ГОСТ 34.003-90. Компонент автоматизированной системы – это часть автоматизированной системы, выделенная по определенному признаку или совокупности признаков и рассматриваемая как единое целое. В контексте настоящей Методики рассматриваемые типы компонентов информационной системы представлены в таблице 1.

Если показатель, характеризующий возможность эксплуатации уязвимости нарушителями (E), может принимать несколько значений (например, имеются сведения об эксплуатации уязвимости в реальных компьютерных атаках и имеются сведения о продаже средств эксплуатации (эксплойта)), то итоговой оценке данного показателя присваивается наибольшее из значений.

В случае изменения в Банке данных угроз безопасности информации ФСТЭК России сведений об эксплуатации уязвимости, расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе должен проводиться повторно с учетом всех изменений.

17. Показатель I_{imp} определяется с учетом возможных последствий воздействий, которым может подвергнуться информационная система при эксплуатации уязвимости, по следующей формуле:

$$I_{imp} = h \times H, \text{ где}$$

H - показатель, характеризующий возможные последствия, которые могут наступить в информационной системе при эксплуатации уязвимости;

h – весовой коэффициент для показателя H (значения приведены в таблице 1 настоящей Методики).

Если показатель, характеризующий возможные последствия, которые могут наступить в информационной системе при эксплуатации уязвимости (H), принимает несколько значений (например, нарушение целостности данных и повышение привилегий), то итоговой оценке данного показателя присваивается наибольшее из значений.

В случае изменения условий, которые влияют на последствия эксплуатации уязвимости, расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе должен проводиться повторно с учетом всех изменений.

Значения весовых коэффициентов и оценок показателей, определяющих влияние уязвимости программных, программно-аппаратных средств на информационную систему приведены в таблице 1.

Таблица 1 – Значения весовых коэффициентов и оценок показателей, определяющих влияние уязвимости на информационную систему

№ п/п	Наименование	Весовой коэффициент показателя (*k, l, p, e, h*)	Наименование возможных значений показателя	Значение показателя (*Ki, Lj, Pm, En, Hk*)	Итог (*k* × *Ki*, *l* × *Lj*, *p* × *Pm*, *e* × *En*, *h* × *Hk*)
Данные для расчета показателя I_{infr}					
1	Тип компонента информационной системы, подверженного уязвимости (K)	0,5	Уязвимости подвержены компоненты системы, обеспечивающие реализацию важных процессов (бизнес-процессов), функций, полномочий	1,1	0,55
			Уязвимости подвержены межсетевые экраны	0,9	0,45
			Уязвимости подвержены сетевые устройства и шлюзы	0,9	0,45
			Уязвимости подвержены телекоммуникационное оборудование, система управления сетью передачи данных	0,8	0,4
			Уязвимости подвержены серверы (центральные вычислительные узлы)	0,7	0,35
			Уязвимости подвержены пользовательские устройства (автоматизированные рабочие места)	0,5	0,25
			Уязвимости подвержены системы хранения данных	0,4	0,2
			Уязвимости подвержены другие компоненты	0,1	0,5
2	Количество уязвимых компонентов информационной системы (обеспечивающих реализацию критических процессов, функций, полномочий, межсетевых экранов, сетевых устройств и шлюзов, автоматизированных рабочих мест, серверов,	0,2	Более 70% компонентов от общего числа компонентов в информационной системе	1,0	0,2
			50-70% компонентов от общего числа компонентов в информационной системе	0,8	0,16

№ п/п	Наименование	Весовой коэффициент показателя (k, l, p, e, h)	Наименование возможных значений показателя	Значение показателя (Ki, Lj, Pm, En, Hk)	Итог ($k \times Ki$, $l \times Lj$, $p \times Pm$, $e \times En$, $h \times Hk$)
	телекоммуникационного оборудования, средств защиты информации, систем хранения данных и других компонентов) (L)		10-50% компонентов от общего числа компонентов в информационной системе	0,6	0,12
			Менее 10% компонентов от общего числа компонентов в информационной системе	0,5	0,1
3	Влияние на эффективность защиты периметра информационной системы (P)	0,3	Уязвимое программное, программно-аппаратное средство доступно из сети «Интернет»	1,1	0,33
			Уязвимое программное, программно-аппаратное средство недоступно из сети «Интернет»	0,6	0,18
Данные для расчета показателя I_{at}					
4	Эксплуатация уязвимости (E)	1,0	Эксплуатируется в реальных атаках	0,6	0,6
			Имеются сведения о наличии средств эксплуатации (эксплойта) уязвимости	0,3	0,3
			Отсутствуют сведения об эксплуатации в реальных атаках (наличии эксплойта)	0,1	0,1
Данные для расчета показателя I_{imp}					
5	Последствия воздействий, которым подвергается информационная система при эксплуатации уязвимости (H)	1,0	Выполнение произвольного кода (Arbitrary Code Execution)	0,5	0,5
			Повышение привилегий (Privilege Escalation)	0,5	0,5
			Обход механизмов безопасности (Security Bypass)	0,4	0,4
			Внедрение кода (Code Injection)	0,34	0,34

№ п/п	Наименование	Весовой коэффициент показателя (*k, l, p, e, h*)	Наименование возможных значений показателя	Значение показателя (*Ki, Lj, Pm, En, Hk*)	Итог (*k* × *Ki*, *l* × *Lj*, *p* × *Pm*, *e* × *En*, *h* × *Hk*)
			Получение конфиденциальной информации (Obtain Sensitive Information)	0,3	0,3
			Нарушение целостности данных (Loss of Integrity)	0,3	0,3
			Отказ в обслуживании (DoS)	0,26	0,26
			Перезапись произвольных файлов (Overwrite Arbitrary Files)	0,22	0,22
			Запись локальных файлов (Write Local Files)	0,2	0,2
			Чтение локальных файлов (Read Local Files)	0,18	0,18
			Поддельный пользовательский интерфейс (Spoof User Interface)	0,12	0,12
			Межсайтовый скриптинг (Cross Site Scripting)	0,1	0,1

18. По результатам расчета уровню критичности уязвимости применительно к конкретной системе (*V*) присваивается одно из значений, указанных в таблице 2. Примеры расчета уровня критичности уязвимости представлены в приложении 1 к настоящей Методике.

Таблица 2 – Значения итоговой оценки уровня критичности уязвимости

№ п/п	Итоговая оценка уровня критичности уязвимости	Наименование уровня критичности уязвимости
1	V > 8,0	Критический
2	5,0 ⩽ V ⩽ 8,0	Высокий
3	2,0 ⩽ V < 5,0	Средний
4	V < 2,0	Низкий

19. Пересчет значения уровня критичности уязвимости должен осуществляться на постоянной основе (по возможности автоматизированными средствами) при выявлении новых сведений об уязвимости (например, выпуске

разработчиком обновлений, устраняющих уязвимость, появление в открытом доступе средств эксплуатации уязвимости).

III. ПРИНЯТИЕ МЕР ЗАЩИТЫ ИНФОРМАЦИИ, НАПРАВЛЕННЫХ НА УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

20. В зависимости от уровня критичности уязвимостей программных, программно-аппаратных средств в конкретной информационной системе оператором принимается решение о приоритизации и сроках их устранения.

21. В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящей Методикой присвоен критический уровень, рекомендуется принять меры по их устранению в течение нескольких часов (до 24 часов) с момента проведения такой оценки.

В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящей Методикой присвоен высокий уровень критичности, рекомендуется принять меры по их устранению в течение нескольких дней (до 7 дней) с момента проведения такой оценки.

В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящей Методикой присвоен средний уровень критичности, рекомендуется принять меры по их устранению в течение нескольких недель (до 4 недель) с момента проведения такой оценки.

В отношении уязвимостей программных, программно-аппаратных средств, которым в соответствии с настоящей Методикой присвоен низкий уровень критичности, рекомендуется принять меры по их устранению в течение нескольких месяцев (до 4 месяцев) с момента проведения такой оценки.

22. Уязвимости программных, программно-аппаратных средств могут быть устранены путем установки обновления программного обеспечения, программно-аппаратного средства или принятия компенсирующих организационных и технических мер защиты информации.

23. В случае если уязвимости содержатся в зарубежных программных, программно-аппаратных средствах или программном обеспечении с открытым исходным кодом, решение об установке обновления такого программного обеспечения, программно-аппаратного средства принимается оператором информационной системы с учетом результатов тестирования этого обновления, проведенного в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 года.

24. В случае невозможности получения, установки и тестирования обновлений программных, программно-аппаратных средств принимаются компенсирующие меры защиты информации.

25. Выбор компенсирующих мер по защите информации осуществляется оператором с учетом структурно-функциональных характеристик информационной системы, а также возможных способов эксплуатации уязвимостей программных, программно-аппаратных средств.

Компенсирующими организационными и техническими мерами, направленными на предотвращение возможности эксплуатации уязвимостей, могут являться:

изменение конфигурации уязвимых компонентов системы, в том числе в части исключения предоставления доступа к их функциям, исполнение которых может способствовать эксплуатации выявленных уязвимостей;

ограничение по использованию уязвимых программных, программно-аппаратных средств или их перевод в режим функционирования, ограничивающий исполнение функций, обращение к которым связано с использованием выявленных уязвимостей (например, отключение уязвимых служб и сетевых протоколов);

резервирование компонентов системы, включая резервирование серверов, телекоммуникационного оборудования и каналов связи;

использование сигнатур, решающих правил средств защиты информации, обеспечивающих выявление в системе признаков эксплуатации уязвимостей;

мониторинг информационной безопасности и выявление событий безопасности информации в системе, связанных с возможностью эксплуатации уязвимостей.

_____

Приложение
к Методике оценки уровня
критичности уязвимостей
программных, программно-
аппаратных средств

Примеры расчета уровня критичности уязвимостей программного обеспечения

Пример 1.

1. Исходные данные об уязвимости:

Сведения об уязвимости, содержащиеся на сайте Банка данных угроз безопасности информации ФСТЭК России *https://bdu.fstec.ru/vul/2025-01611*.

Идентификатор: BDU:2025-01611

Описание уязвимости: Уязвимость операционных систем FortiOS связана с некорректным присваиванием привилегий. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, *повысить свои привилегии*.

Базовый вектор уязвимости: по CVSS 3.1:
AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Уровень опасности уязвимости: Высокий уровень опасности (базовая оценка CVSS 3.1 составляет 8,8).

Наличие эксплойта: Данные уточняются.

Эксплуатация в реальных атаках: Данные уточняются.

1.1 Исходя из уровня опасности уязвимости BDU:2025-01611 по CVSS 3.1, показателю I_{cvss} присваивается следующее значение:

$$I_{cvss}=8,8$$

1.2 Исходя из описания уязвимости, показателю последствий воздействий, которым подвергается информационная система при эксплуатации уязвимости присваивается значение «Повышение привилегий (Privilege Escalation)» (*H=0,5*):

$$I_{imp}=1,0\times 0,5=0,5$$

1.3 Исходя из отсутствия сведений о наличии эксплойта и использовании в реальных атаках показателю возможности эксплуатации уязвимости нарушителями присваивается значение «Отсутствуют сведения об эксплуатации в реальных атаках (наличии эксплойта)» ($E=0,1$):

$$I_{at}=1,0\times 0,1=0,1$$

2. Исходные данные об информационной системе:

2.1 Сведения о компонентах информационной системы определены в органе (организации) по результатам проведенной инвентаризации.

Исходя из данных инвентаризации определено:

Тип компонента информационной системы, подверженного уязвимости: межсетевые экраны

$$K = k \times K = 0{,}5 \times 0{,}9 = 0{,}45$$

Количество уязвимых компонентов информационной системы: 10-50%

$$L = l \times L = 0{,}2 \times 0{,}6 = 0{,}12$$

Влияние на эффективность защиты периметра информационной системы: уязвимое программное, программно-аппаратное средство доступно из сети «Интернет».

$$P = p \times P = 0{,}3 \times 1{,}1 = 0{,}33$$

Таким образом, определяется показатель влияния уязвимости на функционирование информационной системы I_{infr}.

$$I_{infr} = k \times K + l \times L + p \times P = 0{,}45 + 0{,}12 + 0{,}33 = 0{,}9$$

3. Расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе V осуществляется с использованием данных, полученных в предыдущих пунктах, по формуле:

$$V = I_{cvss} \times I_{infr} \times \left(I_{at} + I_{imp}\right) = 8{,}8 \times 0{,}9 \times \left(0{,}1 + 0{,}5\right) \approx 4{,}75$$

Таким образом, уровню критичности указанной уязвимости для имеющейся информационной системы присваивается значение «Средний» (2,0 ⩽ V < 5,0).

Пример 2.

1. Исходные данные об уязвимости:

Сведения об уязвимости, содержащиеся на сайте Банка данных угроз безопасности информации ФСТЭК России *https://bdu.fstec.ru/vul/2025-03219*.

Идентификатор: BDU:2025-03219.

Описание уязвимости: Уязвимость контроллера входящего трафика в кластере Kubernetes ingress-nginx связана с недостаточным пространственным разделением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, *выполнить произвольный код* в контексте контроллера.

Базовый вектор уязвимости: по CVSS 3.1:
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Уровень опасности уязвимости: Критический уровень опасности (базовая оценка CVSS 3.1 составляет 9,8).

Наличие эксплойта: Существует в открытом доступе.

Эксплуатация в реальных атаках: Данные уточняются.

1.1 Исходя из уровня опасности уязвимости BDU:2025-03219 по CVSS 3.1, показателю I_{cvss} присваивается следующее значение:

$$I_{cvss}=9,8$$

1.2 Исходя из описания уязвимости, показателю последствий воздействий, которым подвергается информационная система при эксплуатации уязвимости присваивается значение «Выполнение произвольного кода (Arbitrary Code Execution)» ($H=0,5$):

$$I_{imp}=1,0\times 0,5=0,5$$

1.3 Исходя из отсутствия сведений о наличии эксплойта и использовании в реальных атаках показателю возможности эксплуатации уязвимости нарушителями присваивается значение «Эксплуатируется в реальных атаках» ($E=0,6$):

$$I_{at}=1,0\times 0,6=0,6$$

2. Исходные данные об информационной системе:

2.1 Сведения о компонентах информационной системы определены в органе (организации) по результатам проведенной инвентаризации.

Исходя из данных инвентаризации определено:

Тип компонента информационной системы, подверженного уязвимости:

компоненты системы, обеспечивающие реализацию критических процессов (бизнес-процессов), функций, полномочий;

серверы (центральные вычислительные узлы);

пользовательские устройства (автоматизированные рабочие места);

системы хранения данных.

В соответствии с пунктом 15 настоящей Методики в случае, если несколько компонентов информационной системы подвержены уязвимости,

то итоговой оценке компонента информационной системы присваивается наибольшее из значений оценки показателя (K).

$$K = k \times K = 0{,}5 \times 1{,}1 = 0{,}55$$

Количество уязвимых компонентов информационной системы:

более 70% (компоненты системы, обеспечивающие реализацию критических процессов (бизнес-процессов), функций, полномочий);

50-70% (серверы (центральные вычислительные узлы));

10-50% (пользовательские устройства (автоматизированные рабочие места));

10-50% (системы хранения данных).

В соответствии с подпунктом 2.8 настоящей Методики в случае, если несколько компонентов информационной системы подвержены уязвимости, то итоговой оценке компонента информационной системы присваивается наибольшее из значений оценки показателя (L).

$$L = l \times L = 0{,}2 \times 1{,}0 = 0{,}2$$

Влияние на эффективность защиты периметра информационной системы: уязвимое программное, программно-аппаратное средство доступно из сети «Интернет».

$$P = p \times P = 0{,}3 \times 1{,}1 = 0{,}33$$

Таким образом, определяется показатель влияния уязвимости на функционирование информационной системы I_{infr}.

$$I_{infr} = k \times K + l \times L + p \times P = 0{,}55 + 0{,}2 + 0{,}33 = 1{,}08$$

3. Расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе V осуществляется с использованием данных, полученных в предыдущих пунктах, по формуле:

$$V = I_{cvss} \times I_{infr} \times \left(I_{at} + I_{imp}\right) = 9{,}8 \times 1{,}08 \times \left(0{,}6 + 0{,}5\right) \approx 11{,}64$$

Таким образом, уровню критичности указанной уязвимости для имеющейся информационной системы присваивается значение «Критический» (V > 8,0).
